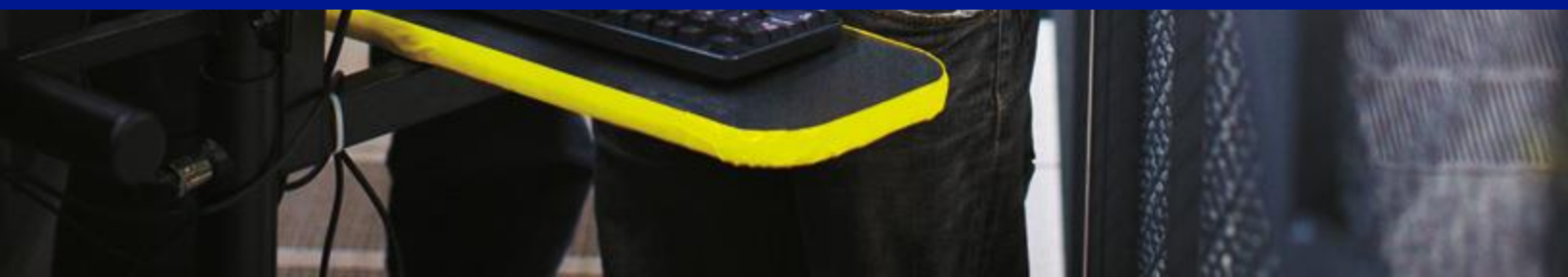
Microsoft

Microsoft Security Intelligence Report

Volume 20 | July through December, 2015

Pakistan



Pakistan

The statistics presented here are generated by Microsoft security programs and services running on computers in Pakistan in 4Q15 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

On computers running real-time security software, most attempts by malware to infect computers are blocked before they succeed. Therefore, for a comprehensive understanding of the malware landscape, it's important to consider infection attempts that are blocked as well as infections that are removed. For this reason, Microsoft uses two different metrics to measure malware prevalence:

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter, whether the infection attempt succeds or not.
- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers executing the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers.

Infection rate statistics for Pakistan

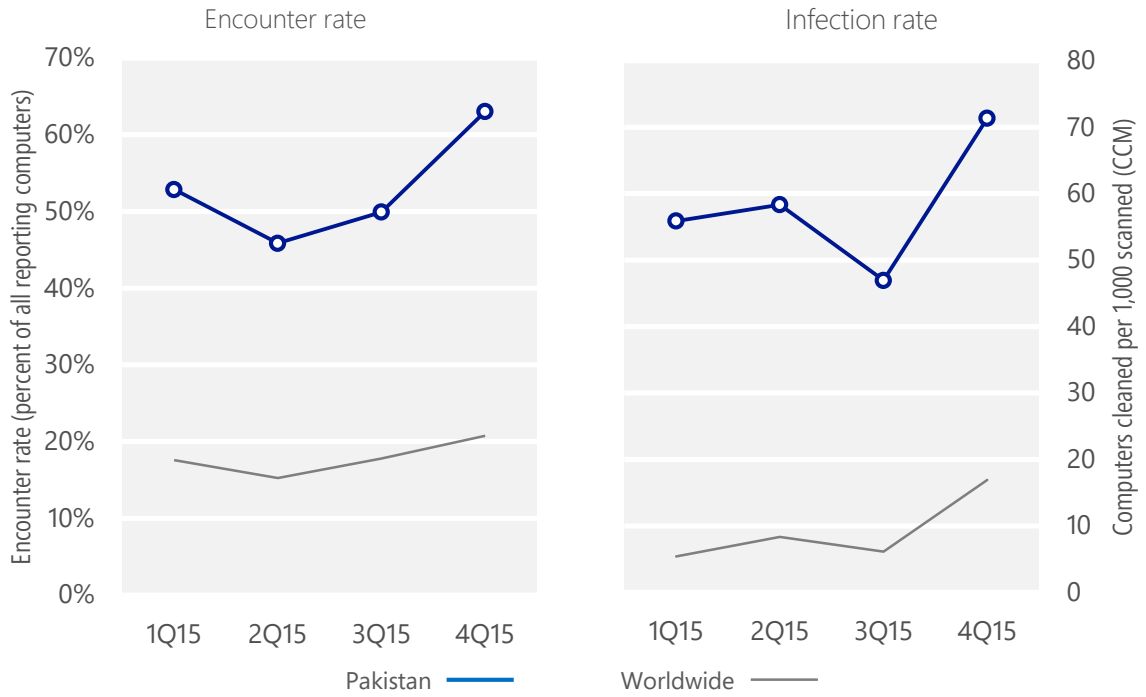
Metric	1Q15	2Q15	3Q15	4Q15
Encounter rate, Pakistan	52.9%	45.9%	49.9%	63.0%
Worldwide encounter rate	*17.6%*	*15.3%*	*17.8%*	*20.8%*
CCM, Pakistan	55.9	58.3	46.9	71.3
Worldwide CCM	*5.4*	*8.4*	*6.1*	*16.9*

Encounter and infection rates reported here do not include totals for the Brantall, Filcout, and Rotbrow malware families. See pages 57–64 of *Microsoft Security Intelligence Report, Volume 17* for an explanation of this decision.

Encounter and infection rate trends

In 4Q15, 63.0% of computers in Pakistan encountered malware, compared to the 4Q15 worldwide encounter rate of 20.8 percent. In addition, the MSRT detected and removed malware from 71.3 of every 1,000 unique computers scanned in Pakistan in 4Q15 (a CCM score of 71.3, compared to the 4Q15 worldwide CCM of 16.9). The following figure shows the encounter and infection rate trends for Pakistan over the last four quarters, compared to the world as a whole.

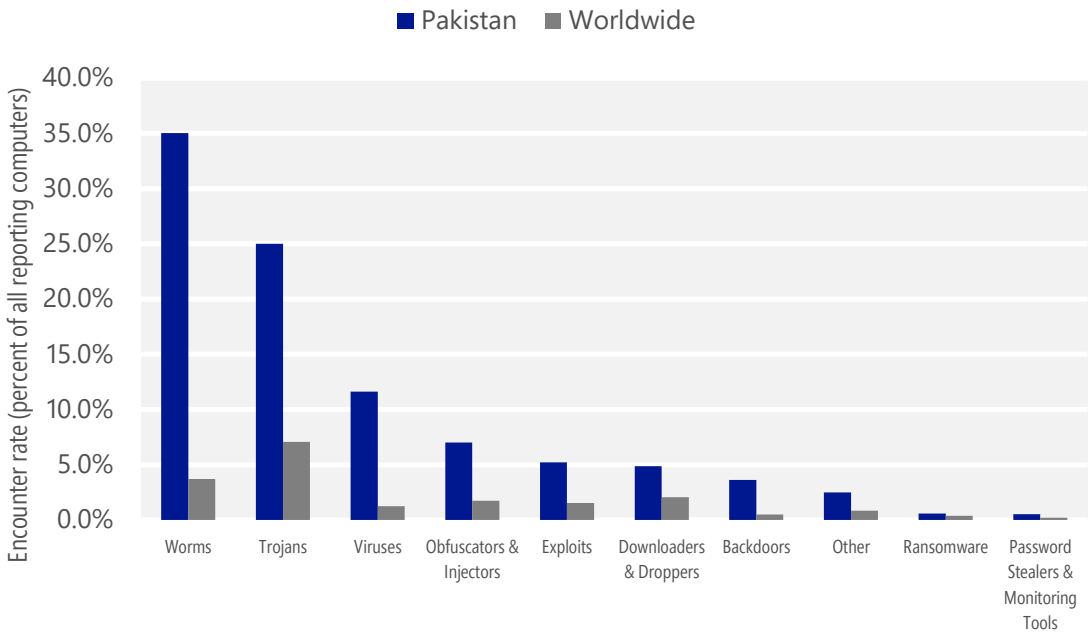
Malware encounter and infection rate trends in Pakistan and worldwide



See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 20* at www.microsoft.com/sir for more information about threats in Pakistan and around the world, and for explanations of the methods and terms used here.

Malware categories

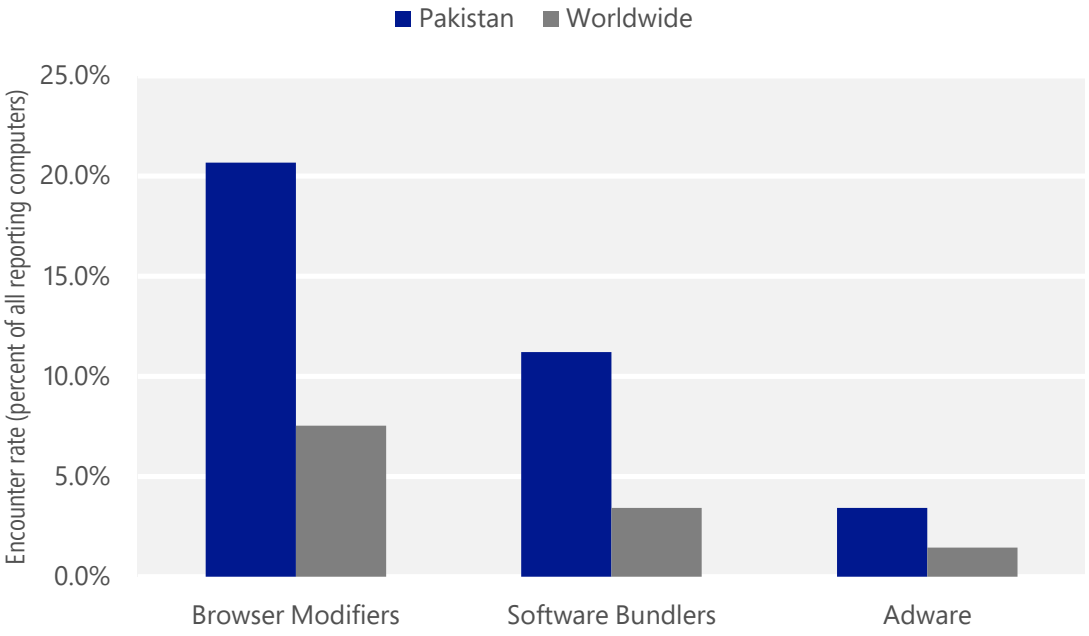
Malware encountered in Pakistan in 4Q15, by category



- The most common malware category in Pakistan in 4Q15 was Worms. It was encountered by 35.0 percent of all computers there, up from 25.6 percent in 3Q15.
- The second most common malware category in Pakistan in 4Q15 was Trojans. It was encountered by 25.0 percent of all computers there, up from 23.3 percent in 3Q15.
- The third most common malware category in Pakistan in 4Q15 was Viruses, which was encountered by 11.6 percent of all computers there, up from 8.5 percent in 3Q15.

Unwanted software categories

Unwanted software encountered in Pakistan in 4Q15, by category



- The most common unwanted software category in Pakistan in 4Q15 was Browser Modifiers. It was encountered by 20.7 percent of all computers there, down from 20.8 percent in 3Q15.
- The second most common unwanted software category in Pakistan in 4Q15 was Software Bundlers. It was encountered by 11.2 percent of all computers there, up from 10.7 percent in 3Q15.
- The third most common unwanted software category in Pakistan in 4Q15 was Adware, which was encountered by 3.4 percent of all computers there, up from 2.8 percent in 3Q15.

Top malware families by encounter rate

The most common malware families encountered in Pakistan in 4Q15

	Family	Most significant category	% of reporting computers
1	Win32/Gamarue	Worms	19.5%
2	Win32/Ippedo	Worms	9.9%
3	INF/Autorun	Obfuscators & Injectors	9.7%
4	VBS/Jenxcus	Worms	8.6%
5	Win32/Nuqel	Worms	6.4%
6	Win32/Sality	Viruses	5.6%
7	Win32/Ramnit	Viruses	4.6%
8	Win32/CplLnk	Exploits	4.3%
9	Win32/Skeeyah	Trojans	4.3%
10	Win32/Chir	Viruses	4.2%

- The most common malware family encountered in Pakistan in 4Q15 was Win32/Gamarue, which was encountered by 19.5 percent of reporting computers there. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The second most common malware family encountered in Pakistan in 4Q15 was Win32/Ippedo, which was encountered by 9.9 percent of reporting computers there. Win32/Ippedo is a worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.
- The third most common malware family encountered in Pakistan in 4Q15 was INF/Autorun, which was encountered by 9.7 percent of reporting computers there. INF/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common malware family encountered in Pakistan in 4Q15 was VBS/Jenxcus, which was encountered by 8.6 percent of reporting computers there. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Top unwanted software families by encounter rate

The most common unwanted software families encountered in Pakistan in 4Q15

	Family	Most significant category	% of reporting computers
1	Win32/SupTab	Browser Modifiers	9.4%
2	Win32/Diplugem	Browser Modifiers	8.6%
3	Win32/OutBrowse	Software Bundlers	4.2%
4	Win32/Mizenota	Software Bundlers	3.1%
5	Win32/Bayads	Adware	2.0%

- The most common unwanted software family encountered in Pakistan in 4Q15 was Win32/SupTab, which was encountered by 9.4 percent of reporting computers there. Win32/SupTab is a browser modifier that installs itself and changes the browser's default search provider, without obtaining the user's consent for either action.
- The second most common unwanted software family encountered in Pakistan in 4Q15 was Win32/Diplugem, which was encountered by 8.6 percent of reporting computers there. Win32/Diplugem is a browser modifier that installs browser add-ons without obtaining the user's consent. The add-ons show extra advertisements as the user browses the web, and can inject additional ads into web search results pages.
- The third most common unwanted software family encountered in Pakistan in 4Q15 was Win32/OutBrowse, which was encountered by 4.2 percent of reporting computers there. Win32/OutBrowse is a software bundler that installs additional unwanted programs alongside software that the user wishes to install. It can remove or hide the installer's close button, leaving no way to decline the additional applications.

Top threat families by infection rate

The most common malware families by infection rate in Pakistan in 4Q15

	Family	Most significant category	Infection rate (CCM)
1	Win32/Diplugem	Browser Modifiers	29.9
2	Win32/Gamarue	Worms	15.2
3	Win32/Sality	Viruses	9.4
4	VBS/Jenxcus	Worms	7.6
5	Win32/Nuqel	Worms	6.1
6	Win32/Chir	Viruses	5.1
7	Win32/Ramnit	Viruses	3.2
8	Win32/Virut	Viruses	3.1
9	Win32/Blakamba	Trojans	2.7
10	Win32/Peals	Trojans	1.3

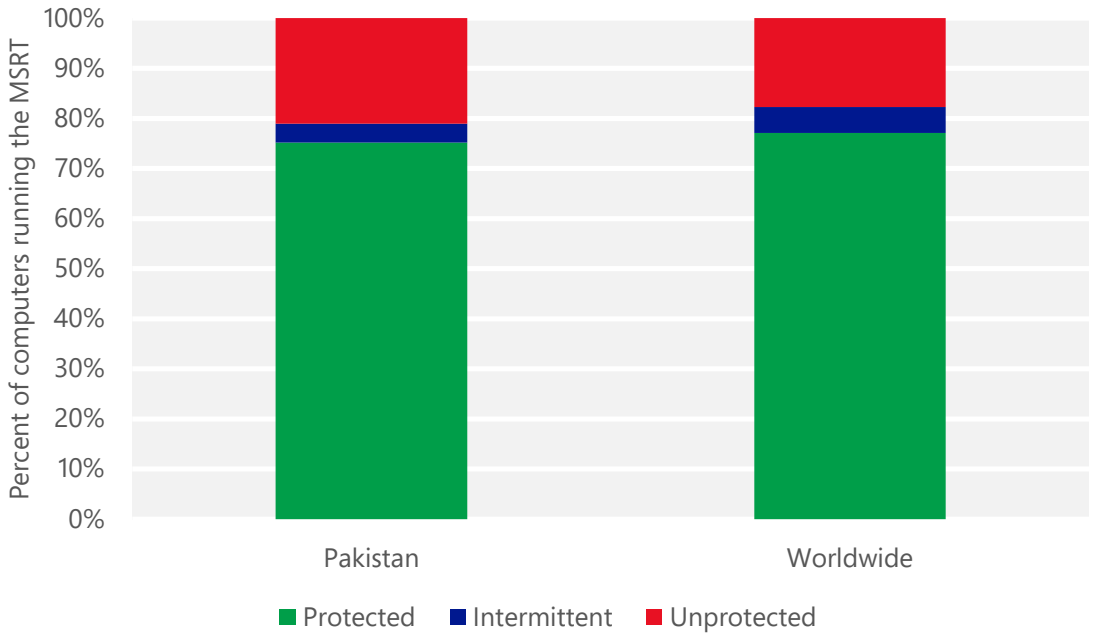
- The most common threat family infecting computers in Pakistan in 4Q15 was Win32/Diplugem, which was detected and removed from 29.9 of every 1,000 unique computers scanned by the MSRT. Win32/Diplugem is a browser modifier that installs browser add-ons without obtaining the user's consent. The add-ons show extra advertisements as the user browses the web, and can inject additional ads into web search results pages.
- The second most common threat family infecting computers in Pakistan in 4Q15 was Win32/Gamarue, which was detected and removed from 15.2 of every 1,000 unique computers scanned by the MSRT. Win32/Gamarue is a worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
- The third most common threat family infecting computers in Pakistan in 4Q15 was Win32/Sality, which was detected and removed from 9.4 of every 1,000 unique computers scanned by the MSRT. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family infecting computers in Pakistan in 4Q15 was VBS/Jenxcus, which was detected and removed from 7.6 of every 1,000 unique computers scanned by the MSRT. VBS/Jenxcus is a worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates.

A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In the figure below, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.

Percent of computers in Pakistan and worldwide protected by real-time security software in 4Q15



Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information presented in this section has been generated from telemetry data produced by the SmartScreen Filter in Microsoft Edge and Internet Explorer. See the Worldwide Threat Assessment section of *Microsoft Security Intelligence Report, Volume 20* for more information about these protections and how the data is collected.

Malicious website statistics for Pakistan

Metric	3Q15	4Q15
Drive-by download pages per 1,000 URLs *(Worldwide)*	0.07 *(0.22)*	0.46 *(0.57)*
Phishing sites per 100,000 Internet users *(Worldwide)*	0.19 *(4.7)*	0.11 *(3.9)*
Malware hosting sites per 100,000 Internet users *(Worldwide)*	38.91 *(56.2)*	11.47 *(26.4)*

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security